



## CodeArmor® Intelligence

### Turnkey Piracy Business Intelligence and Threat Detection and Reporting Tool

New market opportunities, partnerships, and the need for outsourced services is driving Independent Software Vendors (ISVs) and enterprise organizations to continue to deploy valuable software applications into high risk geographies or environments. CodeArmor Intelligence provides a product-based approach that is easily embedded in applications to continually monitor and report on a wide range of threats to software including tampering, piracy and overuse. ISVs can then act on these threats using the detailed information contained in the reports.

### Flexible Threat Detection

The CodeArmor Intelligence product provides a simple Software Development Kit (SDK) that allows software providers to detect and report on a number of threats involving the tampering of application binaries as well as custom events.

### Generates Piracy Leads

In a piracy threat, licensing functions are often disabled using a binary patch or overcome through the use of a key generator. Once piracy is detected, CodeArmor Intelligence is activated to collect specific data and securely report it for notification and action by the ISV. The ISV is then able to identify the organizations using the unlicensed software through actual usage data to aid in license recovery efforts. The CodeArmor Intelligence system provides ISVs a simply and scalable way to gather and report on infringement data from their deployed applications without impacting licensed customers.

### Easy Access to Data

CodeArmor Intelligence allows organizations to view, manage, and report on tampering or other custom events and infringement data without complex and expensive infrastructure. CodeArmor Intelligence provides a dashboard leveraging Force.com's cloud infrastructure to enable a simple and secure way to view, manage and access data.

### System Overview

CodeArmor Intelligence includes:

**Integration SDK** – Provides the programming interface and configuration utilities to add CodeArmor Intelligence to existing software application binaries and configure its stealth reporting technology.

**Web Gateway** – A Java-based server that decrypts, filters, and augments data collected from instrumented applications and logs the data into an extensible file or sends the data to the CodeArmor Intelligence for Salesforce.com plug-in.

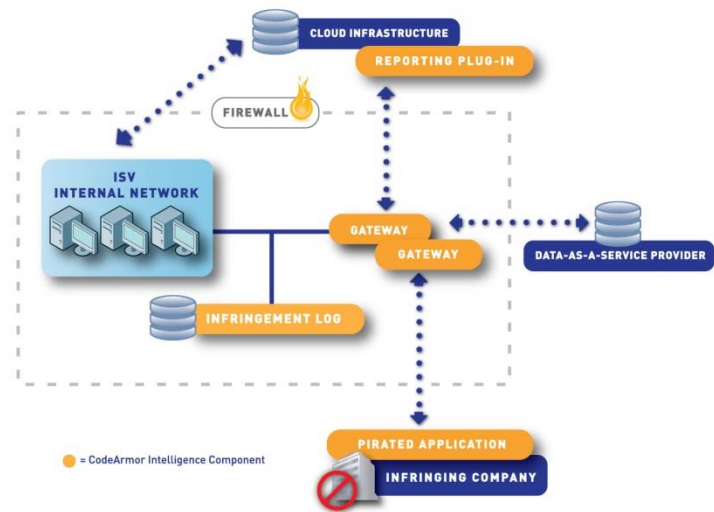
**Reporting Interface Using Force.com** – Provides custom reports, dashboard, and data management capabilities to allow vendors to access piracy data through the Salesforce.com web interface.

### CodeArmor Intelligence at a Glance

- **Piracy Business Intelligence**  
Quantifies piracy adoption and create leads on businesses using unlicensed software
- **Turnkey system**  
Provides an SDK for application integration, central gateway server and a flexible Web reporting interface to implement a threat detection and reporting system
- **Non-intrusive operation**  
Does not impact application performance and runs transparently to detect threats and collect data

## How It Works

The ISV embeds the CodeArmor Intelligence functionality into its application using a flexible SDK. When the application encounters a threat (e.g., tampering), CodeArmor Intelligence's reporting capability activates, collects specific information from the host environment, and communicates the data securely to one or multiple Web gateways configured within the ISV's network. The Web gateway decrypts, filters, and optionally augments the data using third party data-as-a-service providers and then posts it securely to the CodeArmor reporting interface built on Force.com platform. The gateway can use conditional filtering to further tune data being reported or exclude data based on customizable criteria (e.g. certain geographies, or data with less detail). The reporting interface provides ISVs with an easy way to organize, filter, and report on the collected data. In addition, ISVs can use dynamic notification to configure the application to unauthorized use. Alternatively, the ISV can access the Gateway egress data log to integrate the information within an internal CRM or reporting solution.



### FEATURES

### BENEFITS

#### Flexible SDK

- Allows developers to activate and customize CodeArmor Intelligence on a variety of threat scenarios. Detection and reporting library supports 32 and 64-bit Windows and Linux deployments.

#### Non-intrusive runtime

- Transparently egresses forensic data to minimize detection and not impact application flow

#### Conditional filtering

- Gateway can filter data based on conditional rules (e.g. exclude data from specific regions)

#### Dynamic notification

- Triggers an appropriate message or response when software is being used illegally, including alerting or altering the behavior of the unlicensed application

#### Central gateway server

- Allows data to be securely reported back to the vendor's network and centrally filtered
- Egress data is centrally collected in logs to support integration into existing reporting tools

#### Automated location and business profile look-up

- Automatically augments collected data with business profile and geo-location information available through gateway integration with third party data-as-a-service providers

#### Web reporting interface

- Leverages Force.com platform to simplify access to data and create custom dashboards

#### Comprehensive data collection

- Collect application, machine, network, and environment attributes to help identify organizations misusing applications or pinpoint where the application threat was encountered